Non-malleable condensers for arbitrary min-entropy, and almost optimal protocols for privacy amplification.


Summary: Recently, the problem of privacy amplification with an active adversary has received a lot of attention. Given a shared $n$-bit weak random source $X$ with min-entropy $k$ and a security parameter $s$, the main goal is to construct an explicit 2-round privacy amplification protocol that achieves entropy loss $O(s)$. Dodis and Wichs [1] showed that optimal protocols can be achieved by constructing explicit non-malleable extractors. However, the best known explicit non-malleable extractor only achieves $k = 0.49n$ [2] and evidence in [2] suggests that constructing explicit non-malleable extractors for smaller min-entropy may be hard. In an alternative approach, Li [3] introduced the notion of a non-malleable condenser and showed that explicit non-malleable condensers also give optimal privacy amplification protocols. In this paper, we give the first construction of non-malleable condensers for arbitrary min-entropy. Using our construction, we obtain a 2-round privacy amplification protocol with optimal entropy loss for security parameter up to $s = \Omega(\sqrt{k})$. This is the first protocol that simultaneously achieves optimal round complexity and optimal entropy loss for arbitrary min-entropy $k$. We also generalize this result to obtain a protocol that runs in $O(s/\sqrt{k})$ rounds with optimal entropy loss, for security parameter up to $s = \Omega(k)$. This significantly improves the protocol in [4]. Finally, we give a better non-malleable condenser for linear min-entropy, and in this case obtain a 2-round protocol with optimal entropy loss for security parameter up to $s = \Omega(k)$, which improves the entropy loss and communication complexity of the protocol in [2].

Keywords: privacy amplification; non-malleable; extractor; condenser